O

United States District Court
Central District of California

FITSPOT VENTURES, LLC, Plaintiff, v. SOLOMON BIER; and DOES 1–25, inclusive, Defendant.	Case No. 2:15-cv-06454-ODW(RAO) **ORDER GRANTING PLAINTIFF'S EX PARTE APPLICATION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE: PRELIMINARY INJUNCTION [12]**

I. INTRODUCTION

Before the Court is Plaintiff Fitspot Ventures, LLC's Ex Parte Application for a Temporary Restraining Order and Order to Show Cause Re: Preliminary Injunction. For the reasons set forth below, the Court **GRANTS** Plaintiff's Ex Parte Application. (ECF No. 12.)

II. FACTUAL BACKGROUND

Plaintiff Fitspot Ventures LLC (hereafter "Plaintiff" or "Company") is the creator of "Fitspot," a downloadable mobile application that provides its users with on-demand access to fitness trainers and classes (the "App"). (Declaration of Jonathan Cohn ["Cohn Decl."] ¶ 3, ECF No. 12-1.) Upon downloading the App,

customers submit their personal contact and health information through the App's interface. (*Id.*) That information is then used to optimize the customer's experience, both in terms of best training options and so that fitness professionals can present themselves at a customer's training location of choice. (*Id.*) Fitness professionals also provide their personal information through the App's interface, and in turn the trainers are paid through the App for each session that is booked. (*Id.*) Plaintiff takes a fee for each transaction. (*Id.*) Once a customer electronically books a session with a trainer, the trainer immediately receives an "alert" notifying him/her of the customer's name, location, and desired workout, and appointment time. (*Id.* ¶ 4.) The trainer may accept or reject the client's request. (*Id.*) The App's functionality is powered by a set of underlying programming instructions (*i.e.* code) that allow the App to connect customers with trainers. (*Id.* ¶ 5.)

Defendant was invited to join the Company as a coding engineer and held the title of "Technical Co-Founder." (*Id.* ¶ 6.) Defendant's services were rendered in consideration for an equity stake in the Company which was governed by a "Founder's Restricted Unit Agreement" ("FRU Agreement"). (*Id.* ¶ 6, Ex. A.) Concurrently with the FRU Agreement, Defendant also entered into and executed a "Confidentiality and Intellectual Property Assignment Agreement" ("Confidentiality Agreement"). (*Id.*) This agreement specifies that any intellectual property, passwords, marketing strategies, files, certificates, and other computer information would be the exclusive property of the Company. (*Id.* ¶ 7, Ex. B.) It further states that all "Confidential Information" was to be "the exclusive property of [FITSPOT]." (*Id.*, Ex. B.) "Confidential Information" is defined, among other things as "files, keys, certificates, passwords, and other computer information[.]" (*Id.*)

In order to execute his duties, Defendant was provided with a Company issued laptop, monitor, keyboard, and mouse, all of which was purchased by the Company. (Cohn Decl. ¶ 8.) In developing the code for the App, Defendant relied on subscription-based "cloud platforms" to house the underlying source code, and test the

functionality of the App both prior, and subsequent to its release. (*Id.* ¶ 9.) Defendant created accounts with two providers: (1) Heroku; and (2) Github. (*Id.*) Github is a free service, but Heroku is not. (*Id.*) All expenses associated with maintaining the Heroku account were at all times and continue to be paid for by Plaintiff. (*Id.*, Ex. E.) Plaintiff's customer data, proprietary code and App data are all stored in Github and Heroku. (*Id.* ¶ 9.) In addition, the Company uses another digital platform known as Slack. (*Id.* ¶ 11.) Slack is a collaboration tool that facilitates communication between the code repositories (Github and Heroku) and the Company. (*Id.*) If the Heroku or Github accounts are not integrated with Slack, the Company cannot be aware of modifications to the code or bookings from users. (*Id.*)

On August 5, 2015, Plaintiff's CEO, Jonathan Cohn, terminated Defendant's relationship with the Company. (*Id.* ¶ 12.) Cohn requested the return of the Company's tangible and intangible property, including the Company's laptop and other hardware, Plaintiff's code, consumer data, access credentials to the repositories that house the App's code, and access credentials to all other accounts used by Defendant. (*Id.*) After initially refusing to return these items, Defendant returned the Company's laptop, monitor, keyboard, and mouse on August 11, 2015. (Declaration of Maurice Pessah ["Pessah Decl."] ¶ 4, ECF No. 12-2.) However, despite requests to leave data on the laptop unaltered, Defendant wiped the hard drive of the laptop erasing all data that was once stored therein. (*Id.*, Ex. C.) Plaintiff alleges that Defendant has placed all of the data once on the laptop unto a hard drive in Defendant's possession. (*Id.*)

Furthermore, on August 6, 2015, Plaintiff alleges that Defendant accessed Plaintiff's Heroku account and intentionally disabled communication between Plaintiff's Heroku and Slack accounts. As a result, Plaintiff alleges that it is completely cut off from the activities of its customers and therefore deprived of its ability to manage its business. (Cohn Decl. ¶ 11, Ex. F.)

On August 12, 2015, Plaintiff initiated this action in the Superior Court of

California, Los Angeles, against Defendant. On August 14, 2015, Plaintiff filed and was granted an ex parte application for a Temporary Restraining Order (TRO) and an Order to Show Cause Re: Preliminary Injunction. (Mot., Ex. A.) An OSC was scheduled for September 3, 2015, where the State Court would consider the affirmative relief sought by Plaintiff in its TRO application, and rule on whether a preliminary injunction should issue. The State Court ordered Defendant to file an opposition by August 25, 2015. Instead, on that date, Defendant removed the case to this Court. (ECF No. 1.) Plaintiff filed another ex parte application on August 26, 2015. (ECF No. 12 ["Appl."].) Defendant opposed on August 27, 2015. (ECF No. 15.) Plaintiff's Application is now before the Court for consideration.

III. LEGAL STANDARD

A temporary restraining order ("TRO") may issue only if the movant provides specific facts in an affidavit or verified complaint that clearly show "immediate and irreparable injury" will result absent an order. Fed. R. Civ. P. 65(b). The standard applicable to the issuance of a preliminary injunction applies to TROs as well. *Frontline Med. Assocs., Inc. v. Coventry Healthcare Worker's Comp., Inc.*, 620 F. Supp. 2d 1109, 1110 (C.D. Cal. 2009). The movant must establish that (1) it is likely to succeed on the merits; (2) it is likely to suffer irreparable harm in the absence of preliminary relief; (3) the balance of equities tips in its favor; and (4) an injunction is in the public interest. *Winter v. Natural Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008); *Perfect 10, Inc. v. Google, Inc.*, 653 F.3d 976, 979 (9th Cir. 2011). A TRO is "an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief," and it is never awarded as of right. *Winter*, 555 U.S. at 24.

IV. DISCUSSION

A. Likelihood of Success on the Merits

1. Misappropriation of Trade Secrets

To prevail on a claim for misappropriation of trade secrets, a plaintiff must

establish that (1) the information qualifies as a "trade secret," and (2) that the defendant's conduct amounts to "actual or threatened" misappropriation. Cal. Civ. Code § 3426.2(a). "Trade secret" is defined as information, including formula, pattern, compilation, program, device, method, technique, or process that: (1) derives independent economic value, actual or potential, from not being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and (2) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy. *Id*. § 3426.1(d).

Plaintiff argues that Defendant has unlawfully usurped exclusive access to the Company's confidential and proprietary information including: customer information, source code, and access credentials to the source code repositories. (Appl. 15.) Plaintiff further argues that identifying and gathering customers in the Company's target market has cost substantial time and money and that the specific information about a customer's health and fitness goals are of great value to a competing fitness application. (*Id*. 16.) Defendant does not contest that the information is a trade secret.

Courts have consistently found that source code and customer lists are trade secret information. *See Agency Solutions.Com, LLC* v. *TriZetto Group, Inc*., 819 F. Supp. 2d 1001, 1017 (E.D. Cal. 2011) (opining that "source code is undoubtedly a trade secret" under California law); *see also Silvaco Data Sys. v. Intel Corp*., 184 Cal. App. 4th 210, 218 (2010) (disproved on other grounds by *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310 (2010)) (stating that "the source code for many if not most commercial software products is a secret, and may remain so despite widespread distribution of the executable program"); *see, e.g., Courtesy Temp. Serv., Inc. v. Camacho*, 22 Cal. App. 3d 1278, 1288 (1990) (customer list protected as a trade secret where it resulted from a substantial amount of time, expense and effort" and where the "nature and character of the subject customer information is sophisticated information and irrefutable of commercial value and not readily ascertainable to other competitors); *see also Greenly v. Cooper*, 77 Cal. App. 3d 382 392 (1978) ("[A] list of

subscribers of a service, built up ingenuity, time, labor and expense of the owner over a period of many years is property of the employer, a part of the good will of his business and, in some instances, his entire business.").

Furthermore, the Confidentiality Agreement is evidence that Plaintiff treats this information as highly confidential and took reasonable steps to maintain the secrecy of its information. *See Whyte v. Schlage Lock Co.*, 101 Cal. App. 4th 1443, 1454 (2002) (requiring employees to sign confidentiality agreements is a reasonable step to ensure secrecy); *ReadyLink Healthcare v. Cotton*, 126 Cal. App. 4th 1006, 1018 (2005) (employer took reasonable steps to ensure the secrecy of its trade secret information by requesting employees to sign nondisclosure agreements). Defendant does not contest that he entered into the Confidentiality Agreement as a condition of commencing his engagement with Plaintiff. Therefore, the Court finds that Plaintiff will likely be able to show that the information taken by Defendant was a trade secret.

Lastly, Plaintiff will likely succeed in demonstrating that Defendant's conduct threatens disclosure or use of Plaintiff's trade secrets. Plaintiff has provided evidence that Defendant has acted outside the scope of the Confidentiality Agreement by changing the passwords to prevent Plaintiff access to source code and customer information, and maintaining a hard drive with information that was suppose to be turned over to Plaintiff. *See supra*. Furthermore, Plaintiff alleges that Defendant is now working for another tech company, Honk.com, that may benefit from the on-demand and real time functions of the source code. (Appl. 11.) Therefore, the Court finds that Plaintiff will likely succeed in establishing that its customer information and source code qualify as trade secrets and that Defendant's conduct amounts to "actual or threatened" misappropriation.

2. Breach of Written Contract

Plaintiff argues that Defendant entered into a binding written contract with Plaintiff to maintain the secrecy of Plaintiff's confidential and proprietary information and return all proprietary and confidential information and property to Plaintiff.

(Appl. 17.) Moreover, Plaintiff argues that in exchange for an equity stake in the Company, Defendant expressly agreed that all information "concerning the Company's business, technology, business relationships or financial affairs . . . is and will be the exclusive property of the Company" and that "all work performed by [him] would be on 'work for hire' basis." (*Id.*; Cohn Decl. ¶ 7, Ex. A.) As described earlier, Plaintiff has produced evidence that Defendant breached his contractual obligations by preventing access to the source code repositories and maintaining a hard drive with information from his Company laptop.

Furthermore, Defendant does not contest that he has violated the provisions of the contract, but rather that the contracts are void because Defendant was induced to sign the contracts by Cohn's fraud. (Opp'n 2.) Defendant does not provide any evidence for this proposition. Therefore, the Court finds that Plaintiff will likely prevail on its breach of contract claim.

3. Conversion

A claim for conversion arises when one person wrongfully exercises dominion over the property of another. *See Fremont Indem. Co. v. Fremont Gen. Corp.*, 148 Cal.App.4th 97, 119 (2007). Plaintiff argues that Defendant has preserved a copy of data from his Company's laptop; failed to return a computer charger; failed to return $300 parking pass; and failed to return an active Company credit card. (Appl. 18.) Further, Plaintiff argues that Defendant has exclusive possession over the data on the Company's laptop that was copied to an external hard drive, the source code, and the customer data housed on the Heroku and Github accounts. (*Id.*)

Defendant only argues that he also does not have access to the Heroku and Github accounts because they have been frozen due to the TRO issued by the State Court. (Opp'n 8.) While the accounts were frozen due to Plaintiff requesting the TRO, Defendant fails to recognize that Plaintiff instigated litigation because of Defendants actions upon termination. Therefore, the Court finds that Plaintiff will likely prevail on its conversion claim.

B. Likelihood of Irreparable Harm

Plaintiff must demonstrate that it is likely to suffer irreparable injury in the absence of a TRO. *See Winter*, 555 U.S. at 22. Plaintiff argues that because it does not have access to the code repositories, Plaintiff is unable to control the App including repairing "bugs" and "glitches" that are causing the application to fail and accessing its customer data. (Appl. 18.) Plaintiff provides evidence of some of the customer complaints and customers using a competitor application as a result of unaddressed glitches. (*See* Appl. 20–22.) Thus, Plaintiff has shown that it will suffer irreparable harm to its reputation and goodwill. *Herb Reed Enters., LLC v. Florida Entm't Mgmt., Inc.*, 736 F.3d 1239, 1250 (9th Cir. 2013) ("Evidence of a loss of control over business reputation and damage to goodwill" may be sufficient to show irreparable harm.").

C. Balance of Equities

The Court also finds that the balance of equities favors Plaintiff. As described throughout this Order and in Plaintiff's Application, Plaintiff's business has become severely affected by Defendant withholding Plaintiff's trade secrets and intellectual property. (*See, e.g.*, Appl. 12 ("On the evening of August 23, 2015 . . . [c]ustomers, fitness trainers and the Company's officers were unable to login to the App, and business came to a complete standstill.").) Plaintiff has provided a compelling case that according to the Confidentiality Agreement this property never belonged to Defendant in the first place. Therefore, the Court fails to see how returning the information could possibly harm Defendant. Indeed, Defendant never argues any harm. Furthermore, Plaintiff seeks narrow relief, which balances the equities in its favor. *See Bank of Am., N.A. v. Immel*, No. C 10-02483 CRB, 2010 WL 2380877, at *3 (N.D. Cal. June 11, 2010) (finding that plaintiff's narrow relief of seeking only the return of its confidential information and a prohibition on the use of that information by defendants favored plaintiff).

/ / /

D. Public Interest

The Court finds "that the public interest lies in favor of protecting plaintiffs' trade secrets." *Bank of Am., N.A. v. Lee*, No. CV 08-5546 CAS, 2008 WL 4351348, at *7 (C.D. Cal. Sept. 22, 2008). Though California has a strong public policy in favor of vigorous competition, that interest "yields to California's interest in protecting a company's trade secrets." *Id.* (citing *Latona v. Aetna U.S. Healthcare, Inc.*, 82 F. Supp. 2d 1089, 1096 (C.D. Cal. 1999)).

E. Bond

A TRO requires payment of a bond. Fed. R. Civ. P. 65(c). Plaintiff requests that the Court set a bond in the amount that does not exceed $5,000.00. (Appl. 22.) This amount is appropriate in light of the fact that it is Plaintiff's property at issue, and any injury to Defendant is highly unlikely.

V. CONCLUSION

For the reasons discussed above, the Plaintiff's Ex Parte Application for a TRO is **GRANTED**. (ECF No. 12.) Defendant is **ORDERED TO SHOW CAUSE** at **1:30pm on Wednesday, September 9, 2015** in the courtroom of the Honorable Otis D. Wright II, located at 312 North Spring Street, Los Angeles, California 90012, why he, his officers, agents, servants, employees and attorneys and those in active concert or participation with him or them, should not be restrained and enjoined pending trial of this action from:

1. Transacting on or accessing any of code repository accounts used or at one time used by Defendant, to house source code for or in relation to Plaintiff's business known as "Fitspot." This includes the Heroku and Github accounts to which Defendant has had exclusive access since his separation as Technical Co-Founder of Plaintiff's company on August 5, 2015;
2. Using, disseminating, deleting or in any way altering or modifying source code data stored in the code repository accounts (including, but

not limited to, Github and Heroku accounts) that house any data, information or intellectual property related to Plaintiff, its mobile application known as "Fitspot," and any other aspects of Plaintiff's business activities;

3. Using, disseminating, accessing, deleting or in any way altering or modifying Plaintiff's customer data including, but not limited to, customer names, contact information (i.e., emails, phone number and addresses), locations, payment information and number of sessions booked using the Fitspot downloadable mobile application;

4. Using, disseminating, accessing, deleting or in any way altering or modifying Plaintiff's data relating to fitness trainers including, but not limited to, trainer names, locations, payment information and number of sessions booked using the Fitspot downloadable mobile application;

5. Obtaining, using, retaining, accessing, disclosing or disseminating Plaintiff's confidential, proprietary and/or trade secret information stored on any movable memory device in Defendant's possession, custody or control, including, but not limited to, external hard drives and flash drives;

DEFENDANT IS FURTHER ORDERED TO SHOW CAUSE why he, his officers, agents, servants, employees and attorneys and all those in active concert or participation with him or them should not immediately and without delay, deliver the following to Plaintiff's counsel's office at 10100 Santa Monica Blvd., Suite 300, Los Angeles, CA 90067:

1. The company-issued credit card that was given to Defendant while he was rendering services for Plaintiff and acting as an active shareholder of Plaintiff's business;

2. The company-issued parking pass that was given to Defendant while he was rendering services for Plaintiff and acting as Technical Co-Founder of Plaintiff's business;

3. The most recent and active access credentials to the Heroku account that Defendant used in connection with Plaintiff's business up to and including August 5, 2015;

4. All data, source code and programming the Defendant developed for Fitspot while acting as Fitspot's Technical Co-Founder, whether stored in the Heroku account or elsewhere;

5. All data that was at one time stored on, or erased from, the Mac Book Pro laptop computer that Defendant used during his time as "Technical Co-Founder" of Fitspot;

6. All data that was transferred, moved or sent from the Mac Book Pro laptop computer issued by Plaintiff to Defendant while Defendant was acting as Technical Co-Founder of Plaintiff, to the hard drive that was referenced in Defendant's counsel's email to Plaintiff's counsel on August 11, 2015;

7. All of Plaintiff's customer data including, but not limited to, customer names, contact information (i.e., emails, phone number and addresses), locations, payment information and number of sessions booked using the Fitspot downloadable mobile application;

8. All of Plaintiff's confidential, proprietary and/or trade secret information, and intellectual property developed, obtained, accessed or kept by Defendant by virtue of his relationship with Fitspot as its Technical Co-Founder.

PENDING HEARING on the above Order to Show Cause, Defendant, his officers, agents, servants, employees and attorneys and all those in active concert or

participation with him or them **ARE HEREBY RESTRAINED AND ENJOINED** from:

1. Transacting on or accessing any of code repository accounts used or at one time used by Defendant, to house source code for or in relation to Plaintiff's business known as "Fitspot." This includes the Heroku and Github accounts to which Defendant has had exclusive access since his separation as Technical Co-Founder of Plaintiff's company on August 5, 2015;
2. Using, disseminating, deleting or in any way altering or modifying source code data stored in the code repository accounts (including, but not limited to, Github and Heroku accounts) that house any data, information or intellectual property related to Plaintiff, its mobile application known as "Fitspot," and any other aspects of Plaintiff's business activities;
3. Using, disseminating, accessing, deleting or in any way altering or modifying Plaintiff's customer data including, but not limited to, customer names, contact information (i.e., emails, phone number and addresses), locations, payment information and number of sessions booked using the Fitspot downloadable mobile application;
4. Using, disseminating, accessing, deleting or in any way altering or modifying Plaintiff's data relating to fitness trainers including, but not limited to, trainer names, locations, payment information and number of sessions booked using the Fitspot downloadable mobile application;
5. Obtaining, using, retaining, accessing, disclosing or disseminating Plaintiff's confidential, proprietary and/or trade secret information stored on any movable memory device in Defendant's possession,

custody or control, including, but not limited to, external hard drives and flash drives.

IT IS FURTHER ORDERED THAT PENDING HEARING on the above Order to Show Cause, Defendant, his officers, agents, servants, employees and attorneys and all those in active concert or participation with him or them shall immediately and without delay, deliver the following to Plaintiff's counsel's office at 10100 Santa Monica Blvd., Suite 300, Los Angeles, CA 90067:

1. The company-issued credit card that was given to Defendant while he was rendering services for Plaintiff and acting as an active shareholder of Plaintiff's business;
2. The company-issued parking pass that was given to Defendant while he was rendering services for Plaintiff and acting as Technical Co-Founder of Plaintiff's business;
3. The most recent and active access credentials to the Github and Heroku accounts that Defendant used in connection with Plaintiff's business up to and including August 5, 2015;
4. All data, source code and programming the Defendant developed for Fitspot while acting as Fitspot's Technical Co-Founder;
5. All data that was at one time stored on, or erased from, the Mac Book Pro laptop computer that Defendant used during his time as "Technical Co-Founder" of Fitspot;
6. All data that was transferred, moved or sent from the Mac Book Pro laptop computer issued by Plaintiff to Defendant while Defendant was acting as Technical Co-Founder of Plaintiff, to the hard drive that was referenced in Defendant's counsel's email to Plaintiff's counsel on August 11, 2015;

7. All of Plaintiff's customer data including, but not limited to, customer names, contact information (i.e., emails, phone number and addresses), locations, payment information and number of sessions booked using the Fitspot downloadable mobile application;

8. All of Plaintiff's confidential, proprietary and/or trade secret information, and intellectual property developed, obtained, accessed or kept by Defendant by virtue of his relationship with Fitspot as its Technical Co-Founder.

The above Temporary Restraining Order is effective on Plaintiff's filing an undertaking in the sum of **$5,000**. This Order to Show Cause and supporting papers must be served on Defendant no later than **Wednesday, September 2, 2015**. Any response or opposition to this Order to Show Cause must be filed and personally served on Plaintiff's counsel **no later than Friday, September 4, 2015**. Any reply thereto must be filed and personally served on Defendant's counsel no later than **Tuesday, September 8, 2015**.

IT IS SO ORDERED.

September 1, 2015

OTIS D. WRIGHT, II
UNITED STATES DISTRICT JUDGE